ABSTRACT OF THE DISCLOSURE

According to this invention, whether or not information has been tampered with can be detected while authentication information is set to be inseparable from digital information, and original digital data can be restored as long as it is free from tampering.

For this purpose, when authentication information is embedded into digital information input by an image input unit (201), a Hash value calculation unit (202) generates authentication information based on that digital information, an encryption unit (203) encrypts the authentication information using an encryption key, and a digital watermarking unit (204) embeds the encrypted information in the digital information as a digital watermark.